CLAIMS

1. Method for authenticating a user during an attempt to access an entity (6, 7, 8) of a data transmission network (5), which method includes steps in which:

- a terminal (11) transmits to a network (5) entity, an access request (44) containing data for identifying and authenticating the user to the entity, which access request is transmitted by means of the network (5) to an authentication server (16) of the entity,
- the authentication server carries out a procedure for authenticating (28) the user on the basis of identification and authentication data contained in the access request, and
- the authentication server (16) transmits to the user terminal (11) a response message (51) containing the result of the user authentication by the authentication server (16),

characterised in that it also includes steps in which:

- a random number is transmitted to the terminal (11) prior to the transmission of the access request (44),
- data for authenticating the user to at least two entities (6, 7, 8) of the network (5) is calculated using at least one predefined cryptographic algorithm and at least one secret key specific to the user,
- the terminal (11) inserts, into the access request (44), data for identifying the user to said entities of the network (5) and the calculated authentication data, and

- the terminal (11) transmits the access request to an access controller (10) which transmits, to each of the two entities, a respective authentication request (46, 47) containing the data for identifying and authenticating the user to said entities of the network (5), contained in the access request,
- authentication servers (16) of the entities carry out a user authentication procedure (28, 29), on the basis of user identification and authentication data, contained in the authentication requests (46, 47), and
- authentication reports containing results of the authentication procedures carried out by the authentication servers (16) of each of said network entities are transmitted to the terminal (11).

2. Method according to claim 1, characterised in that at least one of the authentication data items is calculated by a module (15) connected to the terminal (11).

3. Method according to claim 1 or 2, characterised in that it includes a preliminary step in which the terminal establishes a connection with a specialized server (12) by means of the network (5), wherein the random number is generated and transmitted to the terminal (11) by the specialized server when the connection has been established.

4. Method according to claim 3, characterised in that the access request (44) transmitted by the terminal is transmitted to the specialized server (12) which inserts therein the random number used to calculate the

authentication data, the access request is then transmitted to the access controller (10) which inserts the random number into the authentication requests transmitted to the two entities (6, 7, 8).

5. Method according to claim 4, characterised in that the authentication procedures carried out by the authentication servers (16) of the entities (6, 7, 8) include a step of searching for the secret key of the user on the basis of the identification data contained in the authentication request, a step of calculating an authentication data item by executing the cryptographic algorithm with the secret key of the user and the random number contained in the authentication request, and a step of comparing the authentication data contained in the authentication request with the calculated authentication data, wherein the user is properly authenticated if the authentication data contained in the authentication request corresponds to the calculated authentication data.

6. Method according to one of claims 1 to 5, characterised in that the entities (6, 7, 8) of the network (5) include a plurality of entities among access providers (6, 7) offering Internet access to the user, IP service providers (8), and an IP transport and access network operator.

7. Method according to one of claims 1 to 6, characterised in that the identification data inserted into the access request (44) is in the form: "IdA@DomainA" in which:

- "IdA" represents the identifier for identifying the user to the network entity,
- "DomainA" represents the identifier of the network entity in the network (5), with the access controller (10) determining the entities to whom the authentication requests (46, 47) will be transmitted on the basis of the "DomainA" identifiers of the network entity contained in the access request (44).

8. Method according to one of claims 1 to 7, characterised in that the steps of authenticating (28, 29) the user by the authentication servers (16) of the entities (6, 7, 8) are carried out in succession.

9. Method according to one of claims 1 to 7, characterised in that the steps of authenticating (28, 29) the user by the authentication servers (16) of the entities (6, 7, 8) are performed substantially simultaneously.

10. Method according to one of claims 1 to 9, characterised in that the random number from which the authentication data is calculated is a random number that is modified in each connection attempt.

11. Method according to one of claims 1 to 10, characterised in that the user authentication procedures are carried out in accordance with the CHAP protocol.

12. System for authenticating a user during an attempt to access an entity (6, 7, 8) of a data transmission network (5) to which network entities are connected, and to which

user terminals can access by means of access networks (1, 2), which system includes:

- means provided in each user terminal for transmitting access requests (44) to an entity of the network, which requests contain data for identifying and authenticating the user to the network entity; and
- at least one authentication server (16) for each of the network entities, designed to identify and authenticate the users according to the identification and authentication data contained in the access requests received,

characterised in that each user terminal (11) includes means for receiving a random number when a connection with the network (5) is established, cryptographic calculating means for applying at least one predefined cryptographic algorithm to the random number received so as to obtain data for authenticating the user to at least two entities of the network (5), and means for inserting, into each transmitted access request (44), data for identifying the user to two network entities and the calculated authentication data, which system also comprises an access controller (10) including means for receiving requests from user terminals and transmitted by the transport network (5), means for extracting, from each of the access requests, the data for identifying and authenticating the user to at least two network entities, and means for transmitting, to each of the two entities, a respective authentication request (46, 47) containing the data for identifying and authenticating the user to the two entities, contained in the access request (44).

13. System according to claim 12, characterised in that it includes an external module (15) designed to connect to each of the user terminals (11) and including means for receiving the random number of the terminal to which it is connected, cryptographic calculation means for executing the predefined cryptographic algorithm based on the random number, and for transmitting, to the terminal, at least one data item for authenticating the user to an entity (6, 7, 8) of the network (5), obtained by the cryptographic calculations

14. System according to claim 13, characterised in that the predefined algorithm is a cryptographic algorithm using a secret key specific to the user and stored by the module (15).

15. System according to claim 13 or 14, characterised in that the module (15) is a smart card, and each terminal (11) comprises means for connecting to a smart card.

16. System according to one of claims 12 to 15, characterised in that the access controller (10) also includes means for receiving user authentication reports (48, 49), transmitted by the entities in response to the authentication requests, and means for transmitting, to the user terminal, and authentication report (51) based on the reports received from the entities.

17. System according to claims 12 to 16, characterised in that it also includes a specialized server (12) connected to the network (5) so as to be connected to the user terminals (11) when a connection has been established

between the terminal and the network, wherein the specialized server includes means for generating and transmitting a random number to each of the terminals with which a connection is established, and means for inserting the random number into each of the access requests transmitted by the terminals.

18. System according to claim 17, characterised in that the specialised server (12) is an HTTP server comprising an interface with the RADIUS protocol.

19. System according to one of claims 12 to 18, characterised in that the access controller (10) is a RADIUS Proxy.

20. System according to one of claims 12 to 19, characterised in that each entity (6, 7, 8) of the network (5) includes means for storing secret keys of users, means for determining the data for authenticating the user to the entity by applying the predefined algorithm to the random number received in the authentication request (46, 47) and to the secret user key, and for comparing the result obtained to the user authentication data received in the authentication request, wherein the user is properly authenticated by the entity only if the result of the cryptographic calculation obtained is identical to the authentication data contained in the authentication request.